NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

CONNECTING OUR NATION'S CRISIS INFORMATION MANAGEMENT SYSTEMS

by

Christopher Voss

December 2008

Thesis Advisor: Richard Bergin
Second Reader: Mel Blizzard

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2008	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Connecting Our Nation's Crisis Information Management Systems		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Christopher Voss			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**	

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT *(maximum 200 words)*

   Many states and localities have implemented Crisis Information Management Systems (CIMS) to integrate situational awareness, notification and disaster assessment tools utilized in Emergency Operation Centers (EOC)s and to eliminate separate stovepipe communications.

   In February 2004, the Department of Homeland Security (DHS) announced the deployment of the Homeland Security Information Network (HSIN) as the primary means for all jurisdictions and levels of government to share information. The system is redundant with state and local CIMS, which have and are being developed.

   Implementing both the integration and interoperability of EOCs requires that the systems used every day be connected; this cannot be achieved through the development of a new system. To implement this solution will require four steps.

- Jurisdictions utilizing CIMS should do more to leverage built in capabilities and jurisdictions without CIMS systems to consider purchasing
- Jurisdictions should integrate the individual information systems currently in use with the jurisdiction's CIMS
- Jurisdictions should improve their systems' abilities to collect and store information
- Jurisdictions should create a portal to allow specific information to be shared across larger regional areas at their discretion and with greater control over who receives the information

14. SUBJECT TERMS Crisis Information Management System; Homeland Security Information Network; Emergency Operation Center; National Incident Management System	15. NUMBER OF PAGES 87
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

i

THIS PAGE INTENTIONALLY LEFT BLANK

CONNECTING OUR NATION'S CRISIS
INFORMATION MANAGEMENT SYSTEMS

Christopher Voss
Director, Montgomery County Office of Emergency Management
and Homeland Security
B.S., University of Connecticut, 1993
M.S., New York Institute of Technology, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2008

Author: Christopher Voss

Approved by: Richard Bergin
                Thesis Advisor

                Mel Blizzard
                Second Reader

                Harold A. Trinkunas, Ph.D.
                Chairman, Department of National Security Affairs

iii

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Many states and localities have implemented Crisis Information Management Systems (CIMS) to integrate situational awareness, notification and disaster assessment tools utilized in Emergency Operation Centers (EOC)s and to eliminate separate stovepipe communications.

In February 2004, the Department of Homeland Security (DHS) announced the deployment of the Homeland Security Information Network (HSIN) as the primary means for all jurisdictions and levels of government to share information. The system is redundant with state and local CIMS, which have and are being developed.

Implementing both the integration and interoperability of EOCs requires that the systems used every day be connected; this cannot be achieved through the development of a new system. To implement this solution will require four steps.

- Jurisdictions utilizing CIMS should do more to leverage built in capabilities and jurisdictions without CIMS systems to consider purchasing

- Jurisdictions should integrate the individual information systems currently in use with the jurisdiction's CIMS

- Jurisdictions should improve their systems' abilities to collect and store information

- Jurisdictions should create a portal to allow specific information to be shared across larger regional areas at their discretion and with greater control over who receives the information

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The number of Federal Disaster Declarations has increased more than seventy percent in the last ten years compared to the previous two decades. This increase, and the increase in size of the U.S. government, has accentuated the criticality of sharing information and coordinating emergency response activities.

Many states and localities have implemented Crisis Information Management Systems (CIMS) to integrate all elements of an agency's response profile (telecommunications, wireless, network, voice, video, and audio) and to eliminate separate stovepipe communications. These systems, for the most part, have been centered in and used by Emergency Operation Centers (EOC)s for the purpose of meeting the requirements laid out in the National Incident Management System (NIMS). Unfortunately, these independent systems were not implemented with a focus on integration across jurisdiction and levels of government, and the nation watched this shortfall manifest itself in the hours and days after landfall. The Hurricane Katrina Lessons Learned stated that DHS should develop and maintain a national crisis communication system to support information exchange from the President, across the Federal government, and down to the State level.[1]

Interestingly enough, the system to support this recommendation was completed one and a half years before Hurricane Katrina made landfall. It was developed to connect federal, state and local jurisdictions. In February 2004, DHS announced the deployment of the Homeland Security Information Network (HSIN) as the primary means for communication, collaboration, situational awareness and information sharing.[2]

---

[1] The White House, "Hurricane Katrina: Lessons Learned," http://www.whitehouse.gov/reports/katrina-lessons-learned/appendix-a.html (accessed October 2008).

[2] Department of Homeland Security, "Homeland Security Information Network," http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm (accessed October 2008).

Unfortunately, the system has not been well received by the emergency management community, and many feel HSIN is redundant with already-developed state and local CIMS.[3]

U.S. EOCs now sit at a precipice where the necessity to promote information sharing is understood, but the implementation of a solution to this problem is in doubt. Even though HSIN is free, emergency managers have given many reasons for the lack of use. These reasons include the following.

- HSIN is not integrated with state-owned and -maintained EOC CIMS systems, resulting in a level of redundancy in reporting
- The system is underused
- There are privacy issues
- The System is not user friendly
- It provides few specifics for many events

So how should the United States implement NIMS, create connectivity across the nation's EOCs and address the lessons learned from the systems before now? This thesis examines why the current method of creating new systems rather than integrating old systems to connect EOCs has not met expectations, and seeks to determine how interoperability and information sharing capabilities might be improved. To accomplish this goal, the following steps were taken.

- Understanding the systems currently being used and how they are being used
- Understanding the limitations or concerns in integrating these systems
- Identifying a set of information criteria to be shared across jurisdictions
- Developing a set of high-level system requirements to improve information sharing

---

[3] Government Accountability Office, "Information Technology, Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives," May 10, 2007, www.gao.gov/new.items/d07822t.pdf (accessed October 2008).

The results conclude that deploying a new system to perform information activities when jurisdictions are already performing the same function internally would result in an additional burden on the end user.[4],[5] The lessons learned from HSIN indicate that the integration of current systems would be better received by Emergency Management personnel and EOC end users.[6] In order to support this solution, this thesis provides a road map by which to connect the systems already in use on a daily basis. To accomplish this task, this paper identifies four critical steps.

- Jurisdictions utilizing CIMS should do more to leverage built in capabilities and jurisdictions without CIMS systems to consider purchasing

- Jurisdictions should integrate the individual information systems currently being utilized with the jurisdiction's CIMS

- Jurisdictions should improve the ability of those systems to collect and store information

- Jurisdictions should create a portal to allow jurisdiction-specific information to be shared across larger regional areas at their discretion and with greater control over who receives the information

Perhaps the failure in previous approaches was in how success was measured. Success in interoperability and integration of the nation's EOC should be measured not as an absolute, but instead as an area that needs to see continuous improvement. It is not connectivity, which is the goal, but rather, an increase in the willingness and degree to which jurisdictions do share. For this reason, the end users' wants and requirements must be considered in developing a system.[7]

Federal, state and local governments should cease trying to find the one system that will work for everyone, and instead seek to improve and connect the information sharing and CIMS already in use every day. This approach will yield both integration and a willingness to use it.

---

[4] Government Accountability Office, "Information Technology, Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives," 1.

[5] Josh Jack, interview with Chris Voss, September 4, 2008.

[6] John Hartwick, "Explaining the Roles of User Participation in Information System Use," *Management Science* 40, no. 4 (1994): 440-465.

[7] Ibid., 440-465.

THIS PAGE INTENTIONALLY LEFT BLANK

I.   INTRODUCTION

Aaron F. Broussard, president of Jefferson Parish in the New Orleans suburbs, stated if "the American government would have responded like Wal-Mart has responded (to Hurricane Katrina), we wouldn't be in this crisis."[8] It is doubtful Mr. Broussard is alone in believing Wal-Mart responded better to Hurricane Katrina than the federal, state and local governments. To understand why some feel this way, one can look at the government's system of information sharing across the country.

Emergency Operations Centers (EOC) are responsible for the coordination of information and resources to support domestic incident management activities, but emergency managers do not know how many EOCs exist in the country.[9] There are hundreds if not thousands of emergency operation centers (EOC) at the local, state and federal government level, and the current information sharing infrastructure connecting these EOCs consists primarily of the use of telephones and e-mails between people who already who each other.

Using the current information-sharing infrastructure, managing large scale incidents requiring successful incident management operations dependent on the involvement of multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines is difficult.[10] These information-sharing difficulties resulted in injury in the aftermath of Hurricane Katrina, as the City of New Orleans was unsuccessful in quickly identifying and allocating resources during response efforts.

---

[8] Michael Barbaro and Justin Gillis, "Wal-Mart at Forefront of Hurricane Relief," *The Washington Post*, September 6, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/09/05/AR2005090501598.html (accessed December 2007).

[9] Department of Homeland Security, *The National Response Plan*, December 2004, www.scd.state.hi.us/documents/nrp.pdf (accessed October 2008).

[10] Department of Homeland Security, Federal Emergency Management Agency, *National Incident Management System*, August 2007, www.nrt.org/Production/NRT/NRTWeb.nsf/AllAttachmentsByTitle/SA-385aNIMS-90-web/$File/NIMS-90-web.pdf (accessed October 2008).

The need to share information with multiple EOCs simultaneously is imperative for a successful response during a catastrophic event. Understanding this need and others, President George W. Bush signed Homeland Security Presidential Directive (HSPD) 8 to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive National Incident Management System (NIMS).[11]

According to NIMS, communications interoperability allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video on demand, in real time, when needed, and when authorized.[12] However, NIMS failed to focus on and develop an information-sharing infrastructure to communicate "across" jurisdictions.

The after-action report for September 11, Hurricane Katrina and two studies (one by the Dartmouth and National Institute for Justice and one by the National Institute for Justice) all provide recommendations on how to bridge the gap between the nation's vision for information sharing between EOCs and its current capabilities. While many of the documents present opinions on how the system can work or be organized, there is not a consensus, most likely because the current literature provides recommendations for specific problems rather than a unified requirements list supported by federal, state and local EOCs.

An argument could be made that the United States has had difficulty in developing a successful information sharing infrastructure as envisioned in Presidential Directives and the National Incident Management System because it has yet to create a model that users at all levels of government find easy to use and useful. The technology solution for this requirement must address user needs and concerns at all levels of government, and not just provide a system in which EOCs *can* share information. Just as important as the ability to share information is the willingness on the part of emergency managers *to* share information.

---

[11] The White House, *Homeland Security Presidential Directive/HSPD-5*, February 28, 2003, http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html (accessed October 2008).

[12] Federal Emergency Management Agency, *National Incident Management System*.

The U.S. government needs to re-think the way it has approached a national information sharing system, which has always been from the top down. Rather than creating new systems and burdens on the emergency management community, this thesis approaches the problem from the bottom up. Specifically, networking individual CIMS should be considered to integrate EOCs and improve information sharing rather than creating a new system. The easiest way for the government to support the capability-specific priorities identified in the national preparedness goals has been to develop a national system, such as the Homeland Security Information Network (HSIN), but with six percent of its HSIN users logging in daily, the system has been too underused to meet current information sharing needs.[13]

This thesis will review the National Incident Management System, which provides high level requirements for information sharing. It will also examine current issues with the previous information sharing systems supported at a national level, and the current systems being used in EOCs today, in order to determine if an opportunity exits to network current systems rather than developing a new system.

---

[13] Hometown Security, "It's a HSIN: the State of Information Sharing," Hometown Security, http://hometownsecurity.blogspot.com/2007/05/its-hsin-state-of-information-sharing.html (accessed September 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

II. RESEARCH OBJECTIVE

The objective of this thesis is to identify how improvements can be made in the information-sharing infrastructure between emergency operation centers (EOC) at all levels of government. How many emergency responders watched Hurricane Katrina devastate New Orleans while receiving most of their information from CNN? With all the funding and focus on emergency management and response, should responders be relying on CNN for information what is going on in a disaster area when this is precisely the type of information that should be produced and disseminated through EOCs?

This thesis will begin with an extensive literature review of the current systems used for information sharing. This review includes documentation of the capabilities and limitations for commonly used information sharing systems, as well as information and opinions on the HSIN.

This thesis will document some of the concerns and oppositions to current systems utilized for information sharing. In addition, the thesis will discuss systems currently being utilized in EOCs, which, if integrated, will create an information-sharing environment more suitable for success by end users.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LITERATURE REVIEW

A. EOCS AND DISASTER TRENDS

President Carter's 1979 Executive Order merged many of the separate disaster-related responsibilities into the Federal Emergency Management Agency (FEMA).[14] John Macy was named as FEMA's first director, and he emphasized the similarities between natural hazards preparedness and civil defense activities.[15] FEMA began development of an Integrated Emergency Management System with an all-hazards approach that included "direction, control and warning systems," which are common to the full range of emergencies.[16] The central facility that was responsible for the systems, as well as communication and coordination, was the emergency operations center (EOC).[17]

EOCs and the systems utilized to share information are necessary for many kinds of emergencies. Possibly the greatest need for these systems occurs with large complex disasters, many of which are given the distinction of a "federally declared disaster." A federally declared emergency requires a governor of a state to ask for federal assistance during an emergency, which requires more support than the combined state and local efforts can bring to bear.[18] The Federal government then reviews the governor's request based on criteria including the following.[19]

- Amount and type of damage (number of homes destroyed or with major damage)
- Impact on the infrastructure of affected areas or critical facilities
- Impacts to essential government services and functions
- Unique capability of federal government

---

[14] Federal Emergency Management Agency, "FEMA History," Federal Emergency Management Agency, http://www.fema.gov/about/history.shtm (accessed November 2007).

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] Ibid.

- Dispersion or concentration of damage
- Assistance available from other sources (federal, state, local, voluntary organizations)
- State and local resource commitments from previous, undeclared events

The effectiveness of an EOC is often judged during these events, when hundreds of personnel flock to an EOC to coordinate the activities of thousands of responders across all levels of government. This was the case with September 11 and Hurricane Katrina. Both events required an enormous amount of collaboration between levels of government. They have also been part of a trend seen during the last ten years, in which there has been a significant increase in the average number of Major Disaster Declarations per year compared to just 20 years ago. The numbers rose from 31.4 declarations per year between 1985 and 1994 to 54.1 declarations between 1998 and 2007, a 72 percent increase.[20]

One reason given for the increase in the number of disasters concerns the difficulty in sharing information. Put simply, government has increased in size, and there are just more pieces to coordinate and information to share with them. Whatever the reason for more declarations, the true size of the federal government increased to 14.1 million workers in 2006[21] from 11 million in October 1999.[22]

The distribution of federally declared disasters across the nation is also not equal. During the period from 1953 to 2008, Texas had more Major Disaster Declarations (81) than any other state, followed by California (73). The District of Columbia, Wyoming, and Rhode Island all had seven major disaster declarations during that same period.

---

[20] Federal Emergency Management Agency, "Major Disaster Declarations," http://www.fema.gov/news/disasters.fema (accessed November 2007).

[21] "Big Government Gets Bigger," *The Washington Post*, October 6, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006100501782.html (accessed October 2008).

[22] Brookings Institute, "Fact Sheet on the New True Size of Government," September 2003, http://www.brookings.edu/articles/2003/0905politics_light.aspx (accessed October 2008).
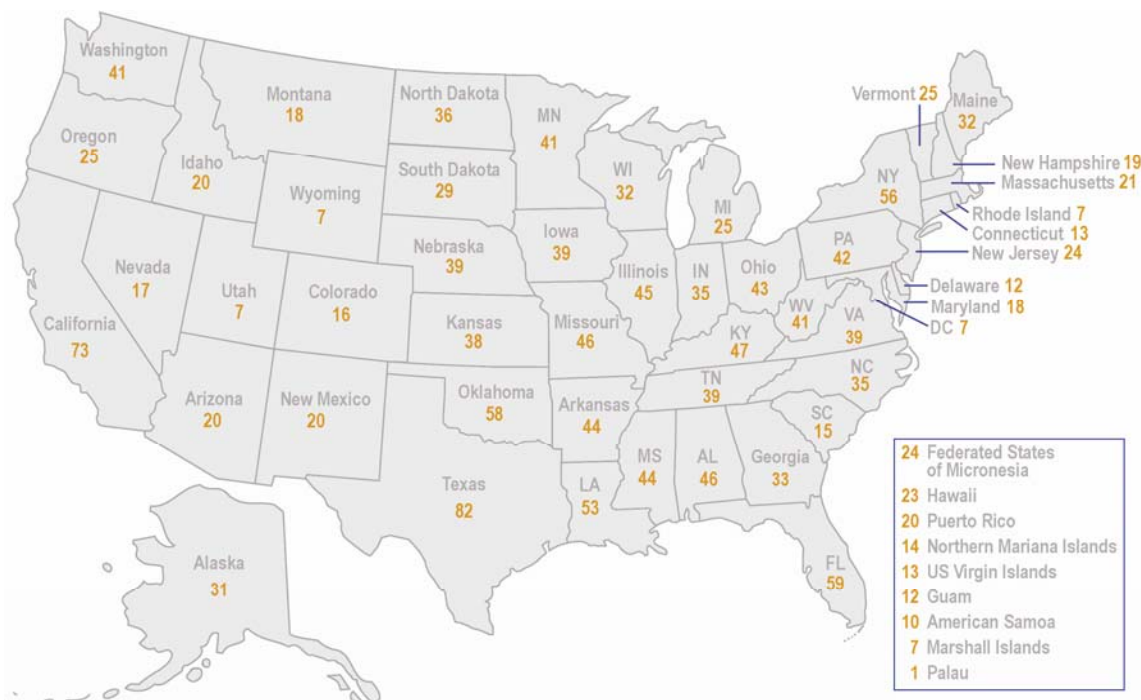
Figure 1.   Number of Federal Disaster Declarations by State[23][24]

Disasters are categorized by state. In fact, according to FEMA, Hurricane Katrina was not one federally declared disaster, but fifty separate disasters.[25] Many of the disaster declarations were given to states and the District of Columbia for their support of evacuees. Coordination and communication between these states' shelters was difficult or completely lacking.[26]   As a result of the lack of coordination during Hurricane Katrina,

[23] Federal Emergency Management Agency, "Major Disaster Declarations," http://www.fema.gov/news/disasters.fema#sev1 (accessed November 2007).

[24] Unpublished Report, EOC Essentials, Johns Hopkins University Applied Physics Laboratory, 2008, 3.

[25] Federal Emergency Management Agency, "Disaster Search Results," http://www.fema.gov/femaNews/disasterSearch.do?pageInfo.pageStart=76 (accessed September 2008).

[26] National Organization on Disability, *Report on Special Needs Assessment for Katrina Evacuees (SNAKE) Project,* 7, http://www.katrinadisability.info/PDFsK/katrina_snake_report.pdf (accessed September 2008).

it was recommended that "DHS should develop and maintain a national crisis communication system to support information exchange from the President, across the Federal government, and down to the State level."[27]

B.   DEFINING CIMS

Many states implemented CIMS to integrate all elements of an agency's response profile (telecommunications, wireless, network, voice, video, and audio) and eliminate separate stovepipe communications networks, which helped promote the use of CIMS systems.[28]   The fundamental objective was to optimize emergency management operations by the use of technology tools that augmented and enhanced the deployment of emergency response assets. In simple terms, emergency managers needed a system that would tie all their systems together.

Areas with larger populations are more likely to utilize CIMS. CIMS programs have been developed to support numerous emergency response actions including the following.

- Asset and resource management
- Emergency GIS data accessibility, interfacing, and/or usage
- Monitoring and data acquisition systems (CBRN sensors, cameras, etc)
- Notification methods and messages
- 911 reporting and dispatch
- Source tasking
- Situation reporting
- Staff, personnel, and organizational management
- On scene situational awareness

---

[27] United States, The White House, *The Federal Response to Hurricane Katrina: Lessons Learned,* (Foreword by Frances Townsend, Assistant to the President for Homeland Security and Counterterrorism), February 23, 2006, http://www.whitehouse.gov/reports/katrina-lessons-learned/appendix-a.html (accessed October 2008).

[28] Department of Justice, National Institute for Justice, *Crisis Information Management Software (CIMS) Feature Comparison Report*, October 2002: 2, http://www.ncjrs.gov/pdffiles1/nij/197065.pdf (accessed November 2007).

- Video camera interfacing

- Preparedness, planning and training

- Accounting and reimbursement

- Data mining and analysis[29]

A survey of current systems by Dartmouth University identified CIMS as both relatively interoperable and interoperable.[30] All of the vendors in the survey said that computers or servers within their CIMS program could share data with each other. The most common method of data transfer used to share data within CIMS programs was the Internet Protocol (IP). The extensible Markup Language or XML was the most common language for the interchange of structured data, and a majority of the systems used XML for both data import and export.[31]

Improving interoperability between EOCs utilizing CIMS has difficulties extending beyond system integration. Perhaps the most significant difficulties involve the willingness to share information between jurisdictions. All CIMS use databases to store data to improve communication and interoperability between these systems; a solution addressing both the integration and social difficulties needed to be found. A major argument for utilizing XML is a reduction in the difficulties associated with integration.[32]

To understand the current environment, one needs to understand that each Emergency Operations Center has been created without the requirement to connect with any other Emergency Operation Center. While some Emergency Operation Centers have created their own CIMS system, others have purchased systems including Blue292, WebEOC, Opscenter, CRISIS, EM2000, E-Team, EOC System, LEADERS, Incident

---

[29] Department of Justice, National Institute for Justice, *Crisis Information Management Software (CIMS) Feature Comparison Report*.

[30] Dartmouth University, Institute for Security Technology Studies, *Crisis Information Management Software (CIMS) Interoperability*, October 2004, http://www.ists.dartmouth.edu/projects/archives/cims1004.pdf (accessed December 2007).

[31] Ibid.

[32] Ibid.

Master, RAMSafe, RESPONSE, RIMS and Softrisk, just to name a few.[33] In addition to there being dozens of different known CIMS options, many states have localities with their own systems.[34] This is critical to understand because, in most instances, even when two EOCs have the same CIMS software, if the systems were not purchased together, they do not have the capability to share information. Therefore, each CIMS supports the EOC it was purchased for and nothing else.

CIMS provides a much more efficient mechanism of accumulating and disseminating information. Many CIMS programs collect information based on the Incident Command System model or the Emergency Support Function Model. By collecting information by sub-category such as "Health" information or "Public Works and Engineering," it allows for easier dissemination to groups interested in only that information, and does not require them to sift through information they do not need. Most CIMS programs allow for the viewing of information as it is being posted. This allows representatives within an EOC as well as other EOCs to view critical information faster.

The 9/11 Commission Report identified a lack of overall awareness as a key challenge for decision makers and responders during the 2001 terror attacks on the United States. Even with the multitude of sensors and communications devices possessed by responder communities, an overall picture of events on the ground was hard to maintain. Many response organizations are deploying CIMS with the specific purpose of helping manage the flow of critical event data.

CIMS have few disadvantages, because they are limited by the lack of integration across jurisdictions and between levels of government. A common architecture for all levels of government to collect information could be developed to form a common operating picture for a multi-jurisdictional response.

---

[33] Department of Justice, National Institute for Justice, *Crisis Information Management Software (CIMS) Feature Comparison Report*.

[34] ESI, "Webeoc Clients," http://www.esi911.com/home/index.php?option=com_content&task=view&id=33&Itemid=44 (accessed October 2008).

C.   CAPABILITIES FOR A NATIONAL CIMS

The current vision for EOCs and how they should share information begins with the NIMS. The purpose of NIMS is to improve emergency management, incident response capabilities, and coordination processes across the country. It is a comprehensive national approach, applicable at all jurisdictional levels and across functional disciplines, and improves the effectiveness of emergency management/response personnel across the full spectrum of potential incidents and hazard scenarios. Such an approach improves coordination and cooperation between public and private agencies/organizations in a variety of emergency management and incident response activities. The NIMS framework sets forth the comprehensive national approach.[35]

The NIMS framework provides guidance on the capabilities of CIMS not just within a jurisdiction, but also across jurisdictions. NIMS also provides many of the capabilities which should be incorporated into EOCs. These capabilities include the following.

- Resource Management
- Interoperability
- Multi-agency coordination
- Creating a Common Operating Picture

1.   Resource Management

Emergency management and incident response activities require carefully managed resources (personnel, teams, facilities, equipment, and/or supplies) to meet incident needs.[36] Utilization of the standardized resource management concepts such as typing, inventorying, organizing, and tracking will facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident. Resource management should be flexible and scalable in order to support any incident and be adaptable to changes. Efficient and effective deployment of resources requires that resource

---

[35] Federal Emergency Management Agency, *National Incident Management System*, August 2007, http://www.fema.gov/library/viewRecord.do?id=2961 (accessed November 2007).

[36] Ibid.

management concepts and principles be utilized in all phases of emergency management and incident response. In the initial stages of an incident, most of the resources requested are addressed locally or through mutual aid agreements and/or assistance agreements. As an incident grows in size or complexity, or if it starts on a large scale, resource needs may be met by other sources.[37]

2. Improving Interoperability

Interoperability between EOCs utilizing CIMS has difficulties extending beyond system integration. Perhaps the most significant difficulties involve the willingness to share information between jurisdictions.[38] All CIMS use databases to store data to improve communication and interoperability between these systems; a solution addressing both the integration and user concerns must be considered. Rather than requiring a jurisdiction to provide access to all it systems and databases, a system that would allow a jurisdiction to control the flow of "its" information with use of a shared space would mitigate the social hesitancy to provide access to unknown organizations and individuals. This structure, including firewalls and protocols between state and local governments, would allow federated searches through a net-centric Information Management system. A major argument for utilizing XML is a reduction in the difficulties associated with integration. Adopting XML means government would not have to junk legacy systems and mainframes, which are very attractive to states that have grown accustomed to their systems and do not have the funding to scrap them.[39] XML makes sharing that information with other entities easy and relatively cheap because it is a web-based technology.

3. Multi-Agency Coordination

The process of multi-agency coordination allows all levels of government and all disciplines to work together more efficiently and effectively. Multi-agency coordination

---

[37] Federal Emergency Management Agency, *National Incident Management System.*

[38] Ibid., 2.

[39] Shane Peterson, "Crime and the Tech Effect, The XML Factor," *Government and Technology*, March 7, 2003, https://www.chds.us/courses/file.php/244/Readings/Winter_07/1-XML_Factor.pdf (accessed November 2007).

occurs across the different disciplines involved in incident management, across jurisdictional lines, and across levels of government. Multi-agency coordination can and does occur on a regular basis whenever personnel from different agencies interact in such activities as preparedness, prevention, response, recovery, and mitigation.[40]

Integral elements of multi-agency coordination systems (MACS) are dispatch procedures and protocols, incident command structure, and the coordination and support activities taking place within an activated EOC. Fundamentally, the many functions of MACS provide support, coordination, and assistance with policy-level decisions to the ICS structure managing an incident(s). A fully implemented MACS is critical for seamless multi-agency coordination activities and is essential to the success and safety of the response whenever more than one jurisdictional agency responds. Moreover, the use of MACS is one of the fundamental components of Command and Management within NIMS, as it promotes the scalability and flexibility necessary for a coordinated response.

4. Common Operating Picture

A common operating picture is established and maintained by the gathering, collating, synthesizing, and disseminating of incident information to all appropriate parties involved in an incident.[41] When responders are supporting a disaster, they often rely on the actions of many others. It is the actions of the collective responders, which produce the overall common operating picture. Achieving a common operating picture allows on-scene responders to see the "big picture." Off-scene responders also gain because they can react to issues or shortfalls in order to limit their impact on the overall response.

One issue identified during Hurricane Katrina was that Secretary Chertoff of Homeland Security lacked up-to-date information on the status of the disaster and the relief effort.[42] One opinion as to why this was an issue was that the Secretary was

---

[40] Federal Emergency Management Agency, *National Incident Management System.*

[41] Ibid.

[42] Association of State and Territorial Health Officials, *A Summary of Four After-Action Reports on Hurricane Katrina*, May 9, 2006, http://www.astho.org/pubs/KatrinaReportsSummary.pdf (accessed November 2007).

unaware of the severity of the incident or shortfalls in the federal government's response and, therefore, could not act to improve or remedy the situation. While infrastructure in many parts of Louisiana and Mississippi was damaged, the inability to connect multiple communications plans and architectures clearly impeded coordination and communication at the federal, state, and local levels.[43]

In the case of Hurricane Katrina, the stakeholders who required knowledge of the common operating procedure included most of the response community. As a result of Hurricane Katrina, reports of evacuees were sent to all fifty states and the District of Columbia, yet these states lacked a common system to easily provide both the federal government and impacted states the number of evacuees they were housing and their locations.[44]

In a survey of emergency managers, the lack of a common operating picture was considered the factor which most influenced decision making.[45] The 9/11 Commission identified a lack of overall awareness as an issue in the emergency response to the terrorist attacks. If everyone is not on the same page, there is little chance senior and elected officials will come to the same conclusions regarding operational decisions. This, in turn, is likely to lead to a lack of continuity across disciplines and jurisdictions.

---

[43] Department of Homeland Security, "Homeland Security Information Network," Department of Homeland Security, 4, http://www.siec.id.gov/meetings/2005/Presentations/Dec_05_HSIN.ppt (accessed September 2008).

[44] Ibid.

[45] National Center for the Study of Preparedness and Catastrophic Event Response (PACER), *Survey of Emergency Management Service Personnel Situational Awareness and Decision Making*, Unpublished Report, 2008.
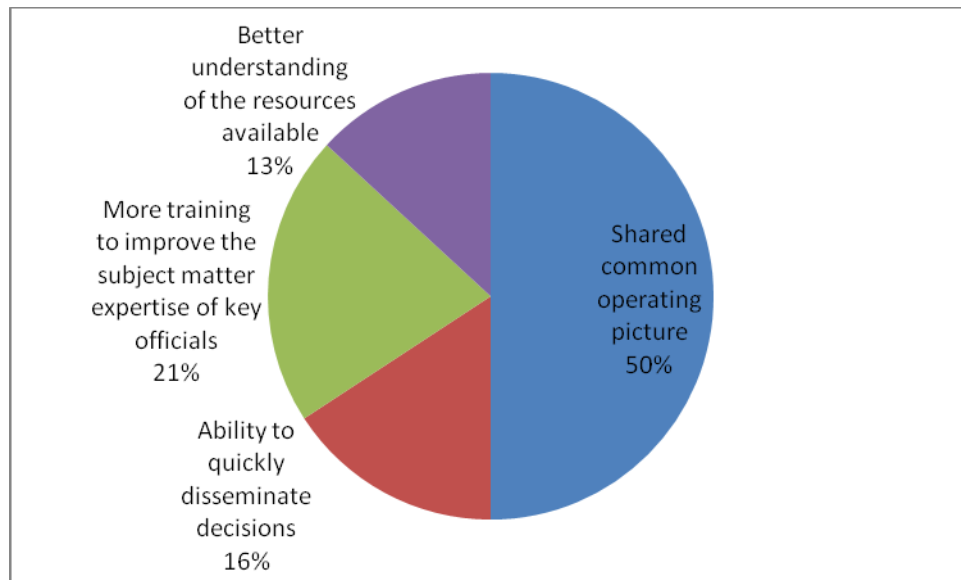
Figure 2.   Factors that have the Greatest Impact on the Decision Making Process Within the Jurisdiction[46]

D.   ONE RING TO RULE THEM ALL

In February 2004, the DHS Secretary announced that HSIN would serve as the primary means for communication, collaboration, situational awareness and information sharing.[47]   Shortly thereafter, the system was deployed throughout the United States. The goal was to provide seamless connectivity throughout the fifty states and to all fifty-three major urban areas for first responder agencies and emergency operation centers.[48] The Department of Homeland Security touted the system as a success during Hurricane Katrina.[49]   At the same time, the development of such a system was identified in Katrina Lessons Learned documents released by the White House as something needing to be done.[50]   How is it possible that the development of a CIMS for the nation was identified as a need when in fact one was in place already?

---

[46] National Center for the Study of Preparedness and Catastrophic Event Response (PACER), *Survey of Emergency Management Service Personnel Situational Awareness and Decision Making*.

[47] Department of Homeland Security, "Homeland Security Information Network," Department of Homeland Security, 4, http://www.siec.id.gov/meetings/2005/Presentations/Dec_05_HSIN.ppt (accessed September 2008).

[48] Ibid., 10.

[49] Ibid., 12.

[50] United States, The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*.

HSIN allows all States and major urban areas to collect and disseminate information among federal, state, and local agencies involved in combating terrorism.[51] In addition, HSIN:

- Helps provide situational awareness

- Facilitates information sharing and collaboration with homeland security partners throughout the federal, state and local levels

- Provides advanced analytic capabilities

- Enables real-time sharing of threat information[52]

For states and locals, HSIN is a low cost system to connect to the federal government and gain access to situation reports, initial action reports, and continuing action reports. Few debate the necessity to have EOCs communicate across the country. HSIN has the ability to meet many of the needs of emergency managers, but the attempt to connect EOCs has been considered a failure by many.[53] Even though HSIN is free, many reasons have been given for the lack of use by emergency managers. These reasons include the following.

- HSIN is not integrated with state-owned and -maintained EOC CIMS resulting in a level of redundancy in reporting[54]

- The system is underused[55]

- There are privacy issues[56]

- The system is not user friendly[57]

- It provides few specifics for many events[58]

---

[51] Department of Homeland Security, "Homeland Security Information Network," 4.

[52] Ibid.

[53] Hometown Security, "It's a HSIN," May 10, 2007, http://hometownsecurity.blogspot.com/2007/05/its-hsin-state-of-information-sharing.html (accessed October 2008).

[54] Ibid.

[55] FCW.com, "Homeland Security Information Network is Underused," http://www.fcw.com/online/news/96059-1.html (accessed September 2008).

[56] Ibid.

[57] Ibid.

[58] Department of Homeland Security, "Homeland Security Information Network," 10.

In one report asking Emergency Managers how HSIN can be improved, the number one concern was its lack of compatibility with other information sharing systems. This same report also identified over 30 percent of the respondents without access to HSIN. This begs the question: How effective can a national system be when almost one third of the emergency personnel do not have access and 40 percent find the system difficult to use?
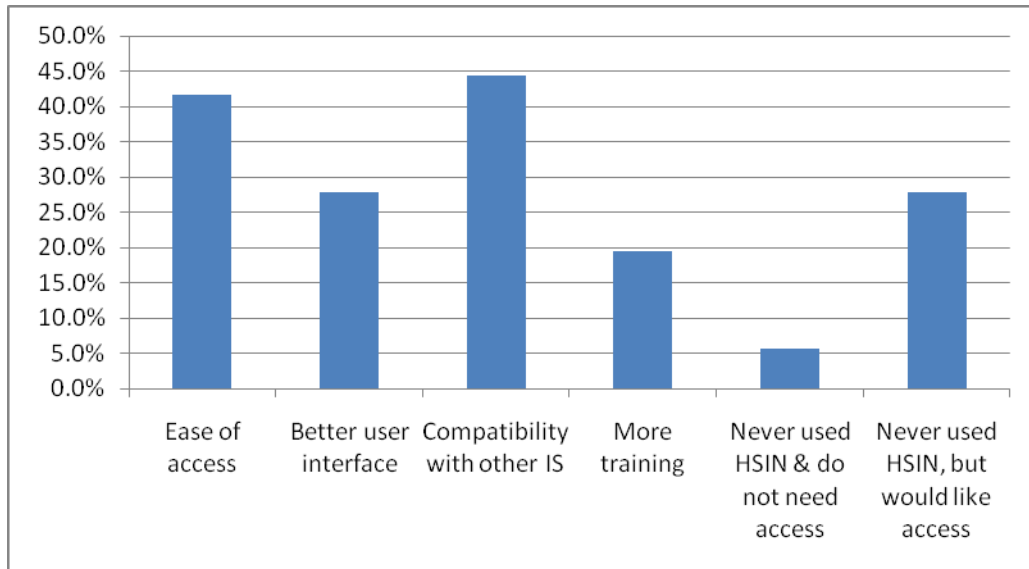
Figure 3.   Factors that can Improve HSIN Usage[59]

As part of the same survey, emergency Managers were also asked, which systems they use for information sharing. The survey was limited and only listed a few systems, but it was notable that the respondents indicated the system they utilized most was a CIMS system typically purchased independently and which can only be found in limited areas across the United States, rather than NIMS, to which most emergency responders have access. The findings also found National Area Warning Alert System (NAWAS) was utilized as much as HSIN. Considering there is typically a single control point in

[59] National Center for the Study of Preparedness and Catastrophic Event Response (PACER), *Survey of Emergency Management Service Personnel Situational Awareness and Decision Making*.

each jurisdiction for this system, unlike HSIN, which can have multiple users within a single jurisdiction, it can be further deduced that HSIN is not being used by a majority of end users.
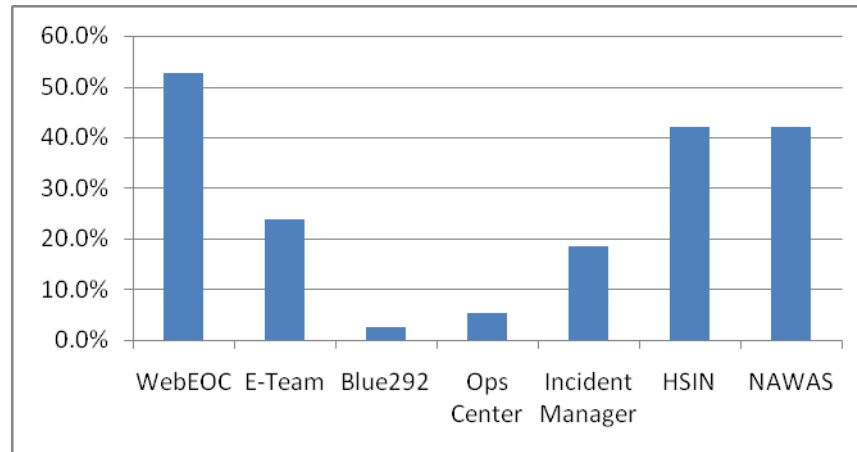
Figure 4.   Usage Distribution of Different Systems for Information Sharing[60]

The Department of Homeland Security has said HSIN needs to be improved because the system "does not provide the necessary capabilities required to provide the necessary trust and interoperability."[61]   Much of the Criticism regarding previous CIMS including HSIN surrounds the concept of trust.   Put simply "Providing the tools/environment and making introductions works better than official mandates because you can't force people to trust people."[62]   Usage of any national system will be partly determined by the trust one user has in other users in other jurisdictions or levels of government.

---

[60] National Center for the Study of Preparedness and Catastrophic Event Response (PACER), *Survey of Emergency Management Service Personnel Situational Awareness and Decision Making*.

[61] FCW.com, "GAO Criticizes HSIN Next Generation Management," http://www.fcw.com/online/news/154048-1.html (accessed October 2008).

[62] Haft of the Spear, "How not to Promote Information Sharing," http://haftofthespear.com/2006/09/how-not-to-promote-sharing/ (accessed October 2008).

IV.   ARGUMENT

The National Preparedness Goal has tasked the government with several capability-specific priorities related to information sharing, including the following.

- Information sharing and collaboration capabilities to enable effective prevention, protection, response, and recovery activities[63]
- Interoperable communications capabilities to enable personnel from different disciplines and jurisdictions to communicate effectively during major events[64]

To enable these specific priorities, knowledge management, information sharing and communication technologies are available, but the public sector has done little to ensure the entire federal, state and local levels of government can manage resources or create a common operating picture during a disaster. The purpose of Homeland Security Presidential Directive (HSPD) 8 is to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive NIMS.[65] Incidents typically begin and end locally and are managed on a daily basis at the lowest possible geographical, organizational, and jurisdictional level. However, there are instances in which successful incident management operations depend on the involvement of multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines.[66] For multiple jurisdictions and agencies to work together to respond to an emergency, it is critical they have the tools to manage emergencies across jurisdictions and not just with other jurisdictions.

To support HSPD 8 and the National Preparedness Goal, a national crisis information management system (CIMS) integrating all elements of an agency's response profile (telecommunications, wireless, network, voice, video, and audio) and eliminating

---

[63] Department of Homeland Security, "Interim National Preparedness Goal," March 31, 2005 http://www.ojp.usdoj.gov/odp/docs/InterimNationalPreparednessGoal_03-31-05_1.pdf (accessed December 2007).

[64] Ibid.

[65] The White House, "Homeland Security Presidential Directive/HSPD-5," February 28, 2003, http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html (accessed December 2007).

[66] Federal Emergency Management Agency, "National Incident Management System."

separate stovepipe communications networks is needed. The fundamental objective is to optimize emergency management operations by the use of technology tools that augment and enhance the deployment of emergency response assets.[67] In simple terms, a national CIMS will allow emergency managers to tie all their systems together and allow them to communicate across jurisdictions.

The Department of Justice and Dartmouth studies appear to be in agreement that each jurisdiction is different and has different needs.[68] For this reason, a national CIMS will need to be flexible, but should utilize a known structure.[69] The national CIMS should also be easily able to the following.

- Integrate with other systems, such as mapping, other CIMS, and telephonic alert notification systems
- Integrate public health into emergency management
- Operate within a variety of network configurations
- Have a wide range of features consistent with the four phases of emergency management[70]

The development of an integrated CIMS has been a top priority articulated by the state and local incident response community to support catastrophic events.[71] The fundamental objective is optimizing emergency management operations by the use of technology tools that augment and enhance the deployment of emergency response assets.

---

[67] Federal Emergency Management Agency, "National Incident Management System."

[68] Department of Justice, *Crisis Information Management Software (CIMS) Feature Comparison Report.*

[69] Dartmouth University, *Crisis Information Management Software (CIMS) Interoperability.*

[70] Ibid.

[71] Department of Justice, *Crisis Information Management Software (CIMS) Feature Comparison Report.*

The United States has not been ignoring the need for the capabilities provided in CIMS, and it may be useful to remember the first rule in providing a technology solution. That rule is that "computer systems can not improve organizational performance if they are not used."[72]

---

[72] Fred Davis, et al., "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* 35, no. 8 (1989).

THIS PAGE INTENTIONALLY LEFT BLANK

V.   SIGNIFICANCE OF RESEARCH

Current documentation is available providing the justification for improved interoperability and information sharing across EOCs; however, the previous approach of having the Department of Homeland Security develop a system and provide a login to States and locals to gain access has proven unsuccessful. The lack of use is not a result of the lack of need, because many EOCs have purchased and are developing their own CIMS.

The significance of this research is to understand why current methods of connecting EOCs have not met users' expectations and determine how their interoperability and information-sharing capabilities may be improved. The research accomplishes this goal by taking the following steps.

- Understanding the systems currently being used and how they are being used

- Understanding the limitations or concerns in integrating these systems

- Identifying a set of information criteria to be shared across jurisdictions

- Developing a set of high level system requirements to improve information sharing

The audience for this thesis includes the federal government, regional and state working groups and Emergency Management Emergency Operation Managers. The value to the audience is not in the individual jurisdiction, but in multiple jurisdictions deciding to take a common approach. It is unlikely that all state, local and federal organizations will agree to the recommendations in this paper at the same time. It is more likely that clusters of jurisdictions will agree to share information and use the recommendations identified in this report. A long-term solution might include multiple clusters, which begin to integrate systems within their emergency operation centers. This paper strives for a time where all CIMS are integrated into what could be described as a "National CIMS," but understands the first step may be "Regional CIMS," defined as multiple states or localities, all with their own CIMS, but integrated with one another.

Success in interoperability and integration of our nation's EOC should be measured not as an absolute, but instead, as an area that needs to see continuous improvement. It is not connectivity that is the goal; the increase in the willingness and degree to which jurisdictions do share is the desired goal. It is for this reason that the end users' wants and requirements must be considered in developing a system. Different audiences will likely use this thesis in different manners.

- Federal Government – The federal government should consider the lessons learned with HSIN and promote regional integration and interoperability. The federal government should also consider national standards and resource typing to facilitate regional implementation.

- State Government – Many states have been purchasing and implementing CIMS for counties and cities within their borders. States should mandate the compatibility of these systems utilizing grant funding. States should also consider the compatibility and connectivity of state systems with adjacent states.

- Local Government – Local jurisdictions should research the systems and capabilities identified within this report and should chose systems based on their area's known hazards. They should communicate those hazards and system capabilities to surrounding jurisdictions, and should encourage the expansion of system capabilities as identified in Chapter IX.

Studies to date have focused on many of the current systems available and how they differ, rather than identifying the requirements by the many users, which could be utilized to improve government's ability to share information across jurisdictions. This report also can be useful to those who support EOCs and are interested in recent surveys, reports and end user opinion on CIMS to support information sharing system development or purchase.

VI.   METHOD

To determine the best approach to improve the EOC-to-EOC information-sharing infrastructure, interviews were conducted with five EOC Directors/Managers at the federal, state and local level. The questions they were asked were designed to support the thesis research questions.

- What systems are currently being used and how?
- What opposition to information sharing between EOCs exists?
- How do the information requirements from EOCs change between jurisdictions and levels of government?
- If a solution does exist, are there cost limitations or considerations to integrating these systems?

The final solution will resemble a model derived by a process modeling method. The goal of process modeling is to explore how people work with the system, taking into account the flow of the activities being performed. Process modeling crosses the boundary of traditional requirements and analysis, and, arguably, even design, because what users will do with the system as well as how the system will support that usage is identified.[73]

As a result of the literature review and interviews with EOC Directors/Managers, a model information-sharing infrastructure was proposed. With any information-sharing technology, resistance of use by end users is critical to success.[74] Seeking to validate the model by end users, a survey of the recommended model was disseminated to determine its level of use over current communication methods. The survey sought to measure the following.

- Ease of use
- Perceived usefulness
- Improved efficiency

---

[73] Agile Modeling, "The Phases of Develop Modeling," 2007, http://www.agilemodeling.com/essays/phasesExamined.htm (accessed February 2008).

[74] Davis, et al., "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," 982.

The Technology Acceptance Model (TAM) has often been studied when determining perceived use. This thesis uses previous reports, interviews, and the literature review and understands factors impacting negative "attitudes" associated with CIMS use.[75] By identifying and mitigating negative attitudes, overall use of CIMS will be improved, and integration and interoperability will be enhanced.

[75] Davis, et al., "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," 982.

VII. A NEW APPROACH TO CONNECTING EOCS

From previous studies and the implementation of HSIN, much has been learned about information sharing between EOCs. Many of these lessons were expensive and time consuming, but in learning what has not worked, one may find an approach more palatable for EOC end users. A future system connecting EOCs should include the following.

- Address trust issues with the federal government
- Be user friendly
- Not create an additional burden for the users

The federal government has taken a top down approach and developed information sharing systems and offered those systems for state and local governments. The result of this approach was HSIN; the concerns around this system were identified in the section titled "One ring to rule them all" (see page 14). Local and state jurisdictions have been purchasing their own CIMS systems to support their daily information-sharing needs and to gain greater control over the information and how it is shared.

One solution addressing the concerns of end users and meeting the daily information-sharing needs of single or multiple discipline response events, as well as rarer complex multiple discipline and multiple jurisdiction events, is to allow the following.

- Jurisdictions to keep their own CIMS systems and jurisdictions without systems to consider CIMS
- Integrate the individual information systems currently being utilized within a jurisdiction with the jurisdiction's CIMS
- Improve the ability of those systems to collect and store information
- Create a portal to allow jurisdiction-specific information to be shared across larger regional areas at the jurisdiction's discretion and with greater control over who receives the information

This approach is not as simple as integrating the systems currently being utilized within a jurisdiction. For integration to be successful, it is first necessary to make sure both that the systems used regularly are a part of CIMS, and that the information has

basic capabilities. Each step in the process is critical, as discussed in this report, and addresses the failures of HSIN and the needs of EOC end users. Table 1 identifies steps needed to achieve a usable, integrated CIMS.

Table 1. CIMS Integration Steps

Step 1	Step 2	Step 3	Step 4
Purchase a CIMS (Most jurisdictions have a CIMS so this step can be ignored by many jurisdictions)	Identify the capabilities within an EOC and integrate those capabilities with CIMS if not already done	Expand information system capabilities to allow all information sharing systems to allow data to be stored, searched, mapped and forwarded	Connect (integrate) individual CIMS to form regional clusters or a national CIMS network
Defining CIMS (Chapter III.B)	Identifying the Pieces (Chapter VII)	Improving the Pieces (Chapter IX)	Connecting all the Pieces (Chapter X)

Although CIMS programs are common and have been valuable in supporting individual Emergency Operation Centers, these programs have not been linked with each other. A study by the National Institute for Justice identified twenty-six different CIMS products being used at the state and local level, and no significant effort is underway for the coordination of these CIMS products and exchange of information between agencies.[76] Various levels of government using different products will continue to be problematic in supporting future disasters, and the use of a federally developed system for State and local EOCs has not been successful.[77]

---

[76] Department of Justice, *Crisis Information Management Software (CIMS) Feature Comparison Report*.

[77] Dartmouth University, *Crisis Information Management Software (CIMS) Interoperability*.

VIII. IDENTIFYING THE PIECES

Many EOCs are currently using CIMS systems, but few use all the capabilities these systems provide. Chapter VII identified many of the capabilities for which a jurisdiction could use its CIMS systems; however, representatives at the federal, state and local level are unlikely to use a majority of those capabilities.[78] Much the same way an office might not use many of the capabilities built into Microsoft Office, these systems have capabilities that are rarely used at all.

This chapter identifies several pieces of software and capabilities that a jurisdiction can integrate with most CIMS systems. Each capability is identified and described along with some of its advantages and disadvantages.

The Washington State EOC was designed to survive and be operational during a major earthquake. The steel-braced and framed building has a base isolation foundation that acts as a shock absorber.[79] The facility, which cost over nine million dollars and is capable of supporting over 100 EOC positions, is a result of the state's risk of earthquake; the funding available and the personnel requirements also contributed to the final EOC design. This EOC has various factors in common with many others, including the fact that personnel, funding, and hazards were primary factors in determining how and what the EOC needed to accomplish. For this reason, it may be difficult to find two EOCs in the country that work in the same way and have the same systems. However, even if there are not two EOCs exactly alike, there are many systems, which can be found in many EOCs. These systems enable each EOC to provide capabilities unique to its area of responsibility. To understand and improve information sharing between EOCs, one needs to consider the systems the EOCs are using currently to perform this function.

The systems many EOCs use now cover a variety of functions. Many of the common systems have been identified below and fall into three different categories. These categories include the following.

---

[78] Josh Jack, interview with Chris Voss, September 4, 2008.

[79] Division of Emergency Management, "Washington State Emergency Operations Center," http://emd.wa.gov/about/emergency_operations_center.shtml (accessed October 2008).

- Notification
- Situational awareness
- Assessment

While these systems are not exhaustive, they represent common capabilities. Each is discussed along with its advantages and disadvantages.

A. NOTIFICATION

The capabilities within an EOC are typically accomplished through a variety of supporting systems (technical and non-technical). The following section focuses on four frequently used technology-based systems: Text Alert, Voice Alert, Sirens, and the Emergency Alert System. No system is able to meet all user needs, so many end users employ multiple systems to support multiple hazards, meet redundancy requirements, and support flexibility in the speed and types of information disseminated.
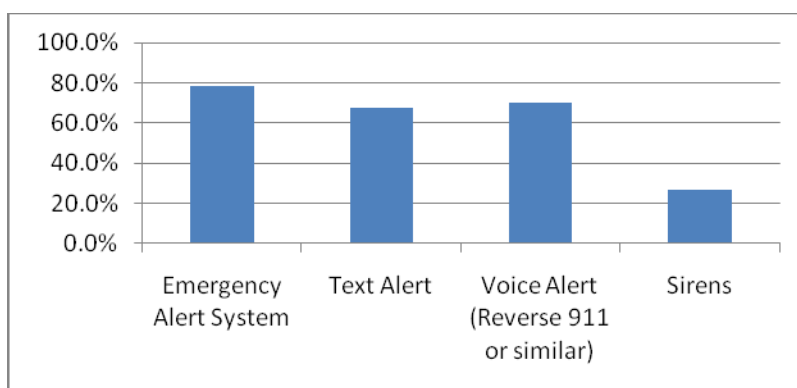
Figure 5.   Percent Use of Notification Systems[80]

1. Text Alert Systems

Text Alert Systems are software applications used to send emergency alerts, notifications, and updates to cell phones, pagers, BlackBerrys, personal digital assistants (PDAs), and/or e-mail accounts.[81] EOCs utilize Text Alert systems to disseminate alerts

---

[80] National Center for the Study of Preparedness and Catastrophic Event Response (PACER), *Survey of Emergency Management Service Personnel Situational Awareness and Decision Making*.

[81] District of Columbia, "Welcome to Alert DC," https://textalert.ema.dc.gov/index.php?CCheck=1 (accessed September 2008).

and updates directly to each cell phone or mobile device. Most systems require individuals to sign up and register devices, subsequently allowing EOCs to notify registered community members of emergencies and provide information and/or directions for protective actions.[82] Many Text Alert systems allow registered community members to create a profile identifying types of information desired and geographic locations of interest.[83] For example, some community members desire traffic or information, and others may desire only weather-relating information. Therefore, the flexibility to choose alert type was viewed as critical and built into many text alert systems.

The capability to provide text messages via a multitude of communication devices (i.e., cell phones, pagers, e-mails), as well as the capability to personalize messages based on community members' preferences, provide flexibility in messaging and mobility that few other notification technologies provide. Text Alert systems are not subject to limitations induced by power failures because most devices operate on batteries; however, it is acknowledged that long-term power outages may limit continued service without the capability to recharge devices or exchange batteries. One challenge for many jurisdictions has been registering community members and their devices, because users must sign themselves up to use this technology.[84]

2. Voice Alert Systems

Voice Alert is a communications solution that uses a combination of database and GIS mapping technologies to deliver outbound notifications.[85] EOC personnel can quickly target a precise geographic area and saturate it with thousands of calls per hour.[86] The system's interactive technology provides immediate interaction with recipients and aids in rapid response to specific needs.

---

[82] Roam Secure, "Citizen Warning System," http://www.roamsecure.net/assets/RSAN%20Cws%20Brochure2.pdf (accessed September 2008).

[83] Ibid.

[84] Montgomery County, "Welcome to Alert Montgomery," https://alert.montgomerycountymd.gov/index.php?CCheck=1 (accessed September 2008).

[85] Reverse 911, "About Reverse 911," http://www.reverse911.com/About_Reverse_911_Part_2_0cb6274.html (accessed September 2008).

[86] District of Columbia Emergency Management Agency, "About Text Alert," http://alert.dc.gov/eic/cwp/view.asp?PM=1&Q=563034&a=3 (accessed May 2008).

A Voice Alert starts in an EOC, when an EOC representative identifies an area to target with a message. The message is then recorded a single time, and that one recording is sent to each local phone carrier customer with a hard-line phone in the designated area. After they have been initiated, most systems will provide the EOC representatives a summary delineating the number of customers called, the number of answering machines that picked up, and the number of phones not answered.

The unique capability of this system is the ability to target localized areas.[87] The capability to provide protective action information to one side of the street and a different set of instructions to another is a valuable tool. Unlike Text Alert, Voice Alert systems do not require action on the part of the community to receive notifications. Anyone with a hard-line phone through the local phone carrier can receive messages. This system also has advantages over several other notification systems in the effectiveness of delivery during evening and late night hours when much of the community may be sleeping and have other notification systems within their home turned off.

Although these systems were created with a geographical interface, some jurisdictions have found significant benefits in their ability to call pre-identified phone numbers. Most systems are flexible enough to input a spreadsheet or database of phone numbers and target this group of people with a single recorded message.

Most Voice Alert systems are limited in the number of phone calls that can be made at one time.[88] This could affect the speed of notification, specifically when alerts need to be disseminated to a large community, because the delivery of the message depends on the number of access lines calling and the length of the recorded message. With more homeowners utilizing cordless phones, this delivery method could be subject to power disruptions, and consideration for customers needing to be accessed through an extension is necessary. With many businesses, hotels, and other locations requiring an extension to reach individuals, the effectiveness of this system could be greatly diminished.

---

[87] Reverse 911, "About Reverse 911."

[88] Dane County, "Dane County Emergency Management Warning Systems," http://www.countyofdane.com/ems/popwarn.htm (accessed September 2008).

One new use for Voice Alert has included the collection of cell phone numbers and Voice Over Internet Protocol (VOIP) numbers for the purpose of dissemination of alerts to those devices via Voice Alert systems.[89] It is also possible to register the number to a specific address, allowing EOC personnel to target alerts to people with cell phones who are interested in receiving information even if they are not in the area of the incident at the time.

3. Siren Systems

Numerous siren systems are now available including those that can provide audible instructions. Most deliver high-intensity warning signals over a large area using omni-directional speakers and are capable of producing a high sound level while making moderate demands on the battery power source.[90] Many are activated by a dedicated radio frequency or phone, and the sirens can be run on batteries charged by a solar panel. Others have AC-only, DC-only, or AC with automatic battery backup operation or solar charging with batteries that allow for continuous operation regardless of power outages. The sound is typically a wail or steady beep.

Siren systems are often used in tornado or tsunami-prone areas because of the speed and reliability with which they can deliver a message.[91] One significant advantage sirens have over other notification methods is that the receiver of the message does not require a TV, pager, computer, phone, etc. to receive the message. Sirens also allow for effective warnings during late night hours or at times when many people may not be near or awake to receive messages from other mechanisms. Considerations for the use of sirens include the lack of flexibility and the cost. Although sirens are being developed that provide verbal instructions similar to a loud speaker, there are few such systems and they have their own set of disadvantages. Most sirens have just a few sound options with little flexibility in the message. Sirens are meant to get the community to do one thing,

---

[89] City of San Diego, Office of Homeland Security, "Reverse 911," http://www.sandiego.gov/ohs/reverse911/index.shtml (accessed October 2008).

[90] Federal Warning Systems, "Omni Directional Siren Systems," http://www.federalwarningsystems.com/products.php?prodid=2 (accessed September 2008).

[91] ATI Systems, "Emergency Warning and Notification Systems," http://www.atisystem.com/applications.htm (accessed September 2008).

such as evacuate or shelter in place. Communities vulnerable to both tornadoes and flash floods would need to be concerned the message they provide does not become misinterpreted and put people in greater danger. This lack of flexibility is the primary reason many organizations choose not to use sirens. The cost to install and maintain sirens could easily exceed the cost of all the other notification technologies discussed.

4. Emergency Alert System (EAS)

The EAS was designed to provide the President with a means to address the American people in the event of a national emergency. Beginning in 1963, the President permitted state and local emergency information to be transmitted using the system.[92] Since that time, local emergency management personnel have used the EAS to relay emergency messages via broadcast stations, cable, and wireless cable systems. While participation in national EAS alerts is mandatory for these providers, state and local EAS participation is currently voluntary.[93]

The EAS allows broadcast stations, satellite radio, cable systems, participating satellite companies, and other services to send and receive emergency information quickly and automatically, even if their facilities are unattended.[94] The EAS was designed to ensure that, if one link in the dissemination of alert information is broken, members of the public have multiple alternate sources of warning. EAS equipment also provides a method for automatic interruption of regular programming and can relay emergency messages in any language.

Along with its capability of providing a national message to the entire public simultaneously, the EAS structure provides authorized users a quick method to distribute important local emergency information. Emergency personnel may use the system to

---

[92] Congressional Research Service, "The Emergency Alert System (EAS) and All-Hazard Warnings," May 5, 2008, www.fas.org/irp/crs/RL32527.pdf (accessed October 2008).

[93] Federal Communication Commission, "Emergency Alert System," http://www.fcc.gov/cgb/consumerfacts/eas.html (accessed September 2008).

[94] Ibid.

disseminate a public warning by broadcasting that warning from one or more major radio stations. EAS equipment in other radio and television stations, as well as cable systems in that state, can automatically monitor and rebroadcast that message.

Additionally, EAS equipment can directly monitor the National Weather Service (NWS) for local weather and other emergency alerts, which local broadcast stations, cable systems, and other EAS participants can then rebroadcast, providing an almost immediate relay of local emergency messages to the public.

Within a jurisdiction, often a few personnel are provided information and access to the EAS system, ensuring that its use meets local criteria for alerting and that it is not overused or abused for non-emergencies. Access into the system through one of these persons is the first step in activating the system.

The EAS is one of the oldest and most relied-upon notification systems. The speed and flexibility in messaging are unique, and only the EAS system can be activated at a national level. It is the only system that broadcasts messages over television and radio. For EAS notification to be successful, those intended to receive the information must be watching or listening to television or radio stations that have agreed to broadcast alerts. During late night hours or work hours, a lower percentage of people can be reached via EAS. In addition, intermittent or power outages obviously reduce its effectiveness.

Table 2.   Notification Systems at a Glance

Notification System	Delivery Method	Advantages	Disadvantages
Text Alert	Pager, cell phone, blackberry, e-mail	• Flexibility of Message • Mobile • Speed of message • Network maintained during short term power outages	• Users must activate their own devices • Message length limitations

37

Notification System	Delivery Method	Advantages	Disadvantages
Voice Alert	Hard-line phones	• Ability to target a specific geographic area • Effective in late night and evening hours	• Must be in close proximity to hard-line phone • Vulnerable to power failures • Delivery speed for large impacted communities • Does not work when "extensions" need to be dialed
Emergency Alert System	Television, radio	• Flexibility of Message • Speed of message	• Community must have devices on and be listening/ watching • Vulnerable to power failures
Sirens	Outdoor speakers and/or sirens	• Speed of message • Effective in late night and evening hours • Reduced effectiveness for people indoors	• Cost • Little flexibility in message • Community must have greater level of training

B.   SITUATIONAL AWARENESS

EOCs use several systems to keep situationally aware of incidents within their jurisdictions. Because of the significant variation in the systems EOCs use, this paper captures common systems found throughout the United States that provide situational awareness, including the National Warning System (NAWAS), Domestic Events Network (DEN), traffic cameras, and syndromic surveillance systems. The following subsections describe these systems and their advantages and disadvantages for situational awareness.

1. **National Warning System (NAWAS)**

NAWAS is a communications system originally designed and implemented in the 1950s as a means of notifying and preparing for a nuclear attack.[95] Fortunately, the United States never has had to use the system for its intended purpose, but it has proven invaluable to local emergency managers responding to or coping with natural disasters.

The NAWAS supports nonmilitary actions taken by federal agencies, the private sector, and individual citizens to meet essential human needs; to support the military effort, to ensure continuity of Federal authority at national and regional levels, and to ensure survival as a free and independent nation under all emergency conditions, including a national emergency caused by threatened or actual attack on the United States.

The NAWAS has major terminals at each state EOC and state Emergency Management Facility. Today, the system consists of what is effectively a telephone party line with more than 2200 members.[96] The phone instruments are designed to provide protection against lightening strikes so they may be used during storms. The interconnecting lines are provided some protection and avoid local telephone switches. This ensures they are available even when a local system is down or overloaded.

Local officials use the system thousands of times a year for emergency management coordination and response. One typical scenario is the use of the system during tornadoes. As storms are sighted, emergency managers in one town or county can communicate with their colleagues in other counties who are in the path of the storm, advising them as to direction, speed, and intensity. Both the National Warning Center (NWC) and the Alternate National Warning Center (ANWC) at Olney, MD are staffed twenty-four hours per day and serve as the primary control for the NAWAS.[97]

---

[95] Louisiana Homeland Security, "National Warning Systems Facts," http://www.ohsep.louisiana.gov/factsheets/nawasfacts.htm (accessed September 2008).

[96] Ibid.

[97] Louisiana Homeland Security, "National Warning Systems Facts."

A key advantage to the NAWAS system is the speed at which information can be disseminated. With thousands of EOCs in possession of NAWAS systems, the ability to ask a question and have it answered by anyone in a number of locations in real time is an enormous benefit. These systems are often used as a way to validate the presence of a hazard quickly and to collect small bits of information for jurisdictional decision-making.

One drawback to this system is that it relies on human intervention. If no one is present to receive the communications, the warning is not disseminated.[98] This has resulted in missed warnings. Many alerts are not stored or recorded, which has sometimes caused information to be distorted because no record is captured of what was said and when. Alerts are all audio, not allowing for easy forwarding of information or the capturing of larger volumes of detailed information.

2.   Domestic Events Network (DEN)

The DEN is a 24/7 Federal Aviation Administration (FAA)-sponsored telephonic conference call network that includes all of the Air Route Traffic Control Centers (ARTCC) in the United States.[99] It also includes various other governmental agencies that monitor the DEN. The purpose of the DEN is to provide timely notification to the appropriate authority that there is an emerging air-related problem or incident within the Continental United States (CONUS). The DEN is managed and facilitated by Air Traffic Security Coordinators (ATSCs) under the direction of Tactical Operations Security.[100] Since several highly publicized airspace violations have occurred over the years, this system has taken a more critical role in providing situational awareness of the nation's airspace.

The DEN provides updates through real-time audio of unfolding air-space violations and the response to the violations. For many state and local organizations with

---

[98] Virtual Museum of the City of San Francisco, "National Warning System Transcript," http://www.sfmuseum.net/quake/nawas.html (accessed September 2008).

[99] Federal Department of Transportation, "Order JO 7210.3v: Facility Operation and Administration," http://www.faa.gov/airports_airtraffic/air_traffic/publications/atpubs/FAC/Ch20/s2004.html (accessed September 2008).

[100] Federal Department of Transportation, "Order JO 7210.3v: Facility Operation and Administration."

access, the system relies on human intervention; and if no one is present to receive the communications, the warning is not received. In addition, the system is not a two-way communication system, so it does not allow jurisdictions to ask questions or users to repeat themselves. State and local governments requesting DEN access are most likely to receive monitoring capability only. The DEN broadcast is not stored or recorded.

3. Traffic Cameras

Understanding traffic within a jurisdiction is critical to support both evacuation and the movement of emergency vehicles to incidents. To provide current traffic awareness, many jurisdictions are providing EOC representatives access to cameras located at key intersections, on major roadways, and on bridges. Although many cameras are focused on roadways, EOC representatives can often provide 360º coverage and potentially provide live video feeds of incidents to responders and strategic decision makers by controlling cameras' movements. Some jurisdictions are integrating hundreds of traffic cameras within a single jurisdiction.

Traffic cameras can provide a real-time assessment of current roadway conditions. This information can be valuable to responders and strategic decision-makers. Often EOCs are provided with access to more traffic cameras than can be viewed simultaneously. Viewing and assessing traffic conditions could be considered burdensome for some jurisdictions.

4. Syndromic Surveillance

The term "syndromic surveillance" applies to surveillance using health-related data that precede diagnosis and signal a sufficient probability of a case or an outbreak to warrant further public health response.[101] Although historically, syndromic surveillance has been utilized to target investigation of potential cases, its utility for detecting outbreaks associated with bioterrorism is increasingly being explored by public health officials.

---

[101] Centers for Disease Control, "Syndromic Surveillance; An Applied Approach to Outbreak Detection," http://www.cdc.gov/ncphi/disss/nndss/syndromic.htm (accessed September 2008).

The foundation of communicable disease surveillance in the United States is the state and local application of the reportable disease surveillance system known as the National Notifiable Disease Surveillance System (NNDSS), which includes the listing of diseases and laboratory findings of public health interest, the publication of case definitions for their surveillance, and a system for passing case reports from local to state to the Centers for Disease Control (CDC).[102] This process works best where two-way communication occurs between public health agencies and the clinical community; clinicians and laboratories report cases and clusters of reportable and unusual diseases, and health departments consult on case diagnosis and management, alerts, surveillance summaries, and clinical and public health recommendations and policies. Although some EOCs receive this information through their health agencies, many do not receive or have not requested the information.

Many states trying to capture a more thorough level of awareness have created systems, in addition to NNDSS, to provide early warning on community-based epidemics. Although this report does not capture all syndromic surveillance systems used by the states, it highlights one for comparison and consideration. The National Capital Region (NCR)—comprising Maryland, Virginia, and the District of Columbia— uses the Early Notification of Community-based Epidemics (ESSENCE) every day. Public health officials use ESSENCE to monitor the health of their populations and to detect disease outbreaks as early as possible to prevent their spread.[103]

To provide public health officials with timely surveillance information, ESSENCE collects and analyzes a variety of health indicator data. For example, ESSENCE gathers data from traditional health indicator sources, such as emergency room visits and over-the-counter drug sales, in addition to several less-traditional sources, such as veterinary visit or water quality data.[104] Once gathered, ESSENCE exhaustively

---

[102] Centers for Disease Control, "National Notifiable Disease Surveillance System," http://www.cdc.gov/ncphi/disss/nndss/nndsshis.htm (accessed September 2008).

[103] Johns Hopkins University Applied Physics Laboratory, "Essence; Protecting Public Health," http://www.jhuapl.edu/newscenter/stories/st050928.asp (accessed September 2008).

[104] Ibid.

analyzes the data using a flexible set of anomaly detection algorithms that produce alerts. These alerts flag unusually high counts of disease indicators that may occur in parts of the population, or sometimes even the population as a whole.[105]

After the data have been analyzed, ESSENCE makes both the processed and the raw data available to public health officials on a secure Web-based platform so that they may perform their routine monitoring and outbreak investigations. ESSENCE offers a variety of tools through with which users can search and visualize the data for themselves, including the following.

- Creating their own charts and graphs of the data

- Generating maps of disease clusters within jurisdictions

- Viewing anonymous details of individual healthcare encounters[106]

- Understanding a jurisdiction's available medical assets and the health of a community by knowing the number of people with serious illnesses and what some of those illnesses are can help decision makers forecast future needs and the possible need for federal assets. Unfortunately, there is not a single syndromic surveillance system utilized across the nation, which adds to the national interoperability difficulties.

5. Geographic Information Systems (GIS)

GIS refers to any system that is capable of integrating, storing, editing, analyzing, sharing, and displaying geographically-referenced information.[107] In a generic sense, GIS is a tool that allows users to create interactive queries (user-created searches), analyze the spatial information, edit data, generate maps, and present the results of all these operations. Many jurisdiction use GIS; however, not all of the participating systems are sufficiently integrated with each other to allow for real-time GIS information sharing.[108]

---

[105] Johns Hopkins University Applied Physics Laboratory, "Essence; Protecting Public Health."

[106] Johns Hopkins University Applied Physics Laboratory, "Medical Surveillance," http://coephi.jhuapl.edu/ESSENCE/ (accessed September 2008).

[107] GIS.com, "A Guide to Geographic Information Systems," http://www.gis.com/whatisgis/index.html (accessed September 2008).

[108] Ibid.

GIS is the industry norm for most jurisdictions. Most EOCs utilize GIS for capturing and storing mapping data within a jurisdiction. The information can be easily accessed and manipulated by EOC personnel. Unfortunately, jurisdictions are required to purchase and maintain GIS systems as well as the asset and facility information embedded within the tools. Considerations should be given to cost and technical expertise to manage and use the systems, which are sometimes more advanced to administer than other mapping systems. One also must consider the continued cost for software and system upgrades.

6. Global Positioning System (GPS)

GPS is funded by and controlled by the U. S. Department of Defense (DOD). While there are many thousands of civil users of GPS worldwide, the system was designed for and is operated by the U.S. military.[109] GPS provides specially coded satellite signals that can be processed in a GPS receiver, enabling the receiver to compute position, velocity and time.[110]

More and more EOCs are incorporating GPS tracking systems to monitor the movement of assets throughout a jurisdiction, including tracking of law enforcement vehicles, fire fighting vehicles, and even heavy equipment to monitor and deploy vehicles for snow removal. Systems often consist of a computer, satellite antenna, and GPS to display the location of host vehicles on the computer's mapping display along with other platforms in their respective locations.[111] The systems, which are similar to Blue Force Tracking but designed for civilian use, can also be used to send and receive messages. As witnessed in one jurisdiction, the GPS tracking system could track the movement of plow trucks, monitor the position of the plow (up or down), calculate the percentage of roadways plowed, and identify roadways still needing to be plowed.

---

[109] Global Positioning system, Global Positioning System Overview, http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html accessed September 2008.

[110] Ibid.

[111] Global Positioning System, "Global Positioning System; Serving the World," http://www.gps.gov/ (accessed September 2008).

GPS tracking offers real-time situational awareness and monitoring of assets, but for some jurisdictions, GPS is cost-prohibitive. Many jurisdictions with this capability will consider it valuable for more than just EOC-supported emergency response activities.

7. Plume Modeling

In a crisis, toxic gas can be released into the air, blocking routes for emergency responders and potentially exposing the community to hazardous conditions.[112] EOCs often use a combination of plume modeling software and information from responders on the ground to identify plumes and predict movement and changes in airborne hazards. Plume modeling computes the spread of toxic gas dispersions that move dynamically with changing wind speed and direction. The software captures weather information either automatically or manually, and allows EOC personnel to input additional variables (including airborne hazard, volumes, and concentrations) to create a dynamic plume geographic map. Such dynamic maps can often forecast future conditions.

One program, Areal Locations of Hazardous Atmospheres (ALOHA)—developed by the Environmental Protection Agency (EPA) Chemical Emergency Preparedness and Prevention Office (CEPPO) and the National Oceanic and Atmospheric Administration (NOAA) Office of Response and Restoration—is part of the agency's Computer-Aided Management of Emergency Operations (CAMEO) suite.[113] Available without cost, it contains a database of approximately 1,000 common chemicals. Using information from this database, including chemical type, accident location (urban or rural), weather conditions (temperature, wind speed, and wind direction), and accident parameters (storage medium, size of opening, pressure of storage medium), ALOHA can predict the

---

[112] Computer Society Digital Library, "Emergency Response Applications: Dynamic Plume Modeling and Real-Time Routing," http://www2.computer.org/portal/web/csdl/doi/10.1109/MIC.2008.11 (accessed September 2008).

[113] Risk World News, "U.S. EPA Updates CAMEO® and ALOHA® Software," http://www.riskworld.com/news/04q3/nw04a106.htm (accessed September 2008).

atmospheric dispersion rate and direction of vapors from a broken pipe, tank, or other source.[114] ALOHA can also generate a visual representation of the plume created by the chemical release.

C.   ASSESSMENT

1.   Hazards U.S. Multi-Hazard (HAZUS-MH)

HAZUS-MH is a risk-assessment software program for analyzing potential losses from floods, hurricane winds, and earthquakes.[115] The FEMA-sponsored system couples current scientific and engineering knowledge with the latest GIS technology to produce estimates of hazard-related damage before, or after, a disaster occurs (http://www.fema.gov/plan/prevent/hazus/).

As FEMA describes it, HAZUS-MH can analyze potential loss estimates, including the following.

- **Physical damage** to residential and commercial buildings, schools, critical facilities, and infrastructure

- **Economic loss**, including lost jobs, business interruptions, and repair and reconstruction costs

- **Social impacts**, including estimates of shelter requirements, displaced households, and population exposed to scenario floods, earthquakes, and hurricanes[116]

HAZUS-MH is an easy-to-use, free software program that can provide a quick analysis of potential damages before windshield surveys are completed and compiled. As occurs with many assessment tools, in some instances, the software has been several orders of magnitude wrong in its assessment. Some EOC personnel consider the system more reliable for hurricanes than other hazards.

---

[114] ESRI, "Emergency Response and Planning Application Performs Plume Modeling," http://www.esri.com/news/arcuser/1003/plume1of2.html (accessed September 2008).

[115] Federal Emergency Management Agency, "HAZUS Overview," http://www.fema.gov/plan/prevent/hazus/hz_overview.shtm (accessed September 2008).

[116] Ibid.

2. Sea, Lake, and Overland Surges from Hurricanes (SLOSH)

SLOSH is a computerized model run by the National Hurricane Center (NHC) to estimate storm surge heights and winds resulting from historical, hypothetical, or predicted hurricanes by taking into account the pressure, size, forward speed, track, and winds of the hurricane.[117] The calculations are applied to a specific locale's shoreline, incorporating the unique bay and river configurations, water depths, bridges, roads, and other physical features. The model can be used to estimate storm surge from a predicted hurricane. The SLOSH model is generally accurate within ± 20 percent of actual storm surge heights and accounts for astronomical tides.[118]

SLOSH is a proven software application that is easy to use and is accurate when determining worst-case scenarios. The software is free of charge and can be easily installed on most computers. Unfortunately, the point of a hurricane's landfall is crucial to determining which areas will be inundated by the storm surge.[119] Where the hurricane forecast track is inaccurate, SLOSH model results will be inaccurate. The SLOSH model, therefore, is best used for defining the potential maximum surge for a location rather than actual storm surge.

---

[117] Federal Emergency Management Agency, "Sea, Lake, and Overland Surges from Hurricanes (SLOSH)," http://www.fema.gov/plan/prevent/nhp/slosh_link.shtm (accessed September 2008).

[118] Ibid.

[119] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

IX. IMPROVING THE PIECES

It is important to "[u]se a system on a daily basis and not just during a crisis."[120] This will be considered an important user requirement and it is one of the reasons emergency managers have purchased CIMS to support their own EOCs.

Somewhere in the development of many information-sharing systems, including HSIN, there may have been a technology push versus a user-driven pull for information. If there had been a user pull, more local emergency managers may be using the system; instead, reports show that daily use is as low as six percent of the total 18,000 registered users.[121] Most of the emergencies localities deal with are small, and the resources to respond to those emergencies are fully provided by the jurisdiction in which the incident is contained, so the need for an additional system to communicate with other jurisdictions is reduced. The tools many emergency managers use to manage these incidents are the systems they are familiar with and use on a regular basis. Use of a system expands the knowledge and comfort users have with that system, and it is the primary factor in the success of a CIMS system. The lack of familiarity is likely to be one of the reasons many feel HSIN is not user friendly.

When emergency managers were asked about the technologies they do use during an incident, it should be no surprise that the two most common answers were telephone and e-mail. When considering system candidates for integration within an EOC, ALL systems must be considered, and not just those that might be core to EOC operations.

---

[120] Lorenzo Jones 3, Interview with Chris Voss, September 9, 2008.

[121] Hometown Security, "It's a HSIN," May 10, 2007, http://hometownsecurity.blogspot.com/2007/05/its-hsin-state-of-information-sharing.html (accessed October 2008).
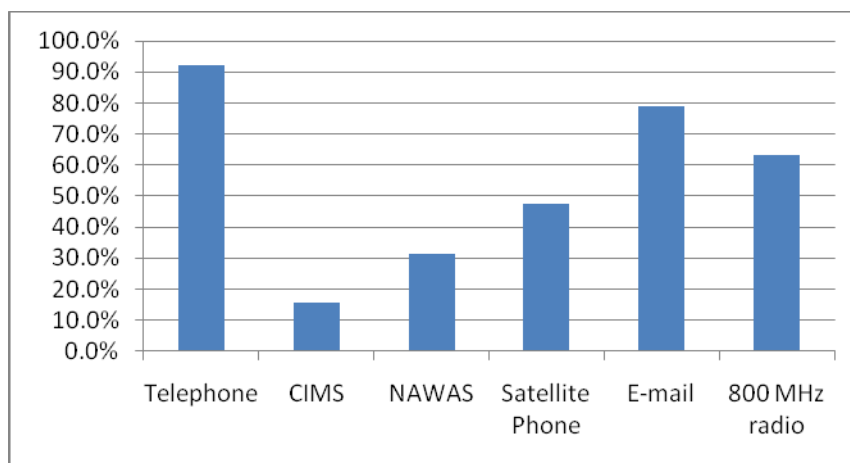
Figure 6.   Utilization of Different Technologies for Collecting and Disseminating Information during an Incident[122]

Additional capabilities could improve the EOC disaster management, and each should include the ability to "search, store, map and forward" information.[123] In Chapter VIII, each system was identified. In Table 3, the communication medium is identified for each and is compared to wanted capabilities.

Ensuring these four capabilities exist with each system may also improve the ability to develop a common operating picture as identified in NIMS. Systems including NAWAS and the DEN consist of voice updates and, if someone is not tuned into the system, the message is not heard. After a call, it might be necessary to check what was said, but the ability to replay is missing. If the information is needed to compile a report or search multiple conversations weeks later, it is generally not available. Each of these capabilities adds to the system and will allow for better management of information versus just sharing of information. "We need to focus on basic capabilities which can be added to our current systems now to improve information management."[124]

---

[122] National Center for the Study of Preparedness and Catastrophic Event Response (PACER), *Survey of Emergency Management Service Personnel Situational Awareness and Decision Making*.

[123] Josh Jack, interview with Chris Voss, September 4, 2008.

[124] Ibid.

Additional capabilities can improve information management by being as follows.

- Searchable – It is often necessary to look at multiple pieces of information and review information for like terms or sort through large volumes of information to target specific information or results

- Stored – The ability to document an incident and operational activities for the purposes of developing situation reports or the development of after action reports is an important process to be followed during and after any incident

- Tied to a location – Many reports either do not identify a specific location for an incident, or identify locations differently, leaving a comparison difficult. The ability to map resources, actions or even what part of a community might have received a specific protective action message is vital in creating a common operating picture

- Easily reproducible or forwardable – In instances where information is being captured, the ability to disseminate beyond a system's "approved users" or beyond a closed system may allow the notification of additional stakeholders

As many of these systems are transferring from older technologies to digital, the ability to expand upon the previous capabilities is also evolving.

Table 3.   System Capability

SYSTEM	INFORMATION DESCRIPTION	COMMUNICATION MEDIA	Capabilities			
			Searchable?	Stored?	Tied to Location?	Easily reproducible/forwarded?
Text Alert	Alert notification utilizing pager, cell phone, blackberry and e-mails	**Text**	N	Y	Y	Y
Voice Alert	Alert notification over hard-line phones	**Voice/Text/ TDY**	N	S	Y	N
Emergency Alert System	Alert notification over television and radio	**Text**	N	N	N	N
Sirens	Alert notification via audio sounds primarily through outdoor speakers and/or sirens	**Audio**	N	N	N	N
NAWAS	Information sharing between surrounding EOCs and between levels of government	**Voice**	N	S	N	N
DEN	Notification of airspace violations and COP of the federal response for that violation	**Voice**	N	N	N	N
Traffic Cameras	Situational awareness of roadway conditions	**Video**	N	N	Y	N

SYSTEM	INFORMATION DESCRIPTION	COMMUNICATION MEDIA	Capabilities			
			Searchable?	Stored?	Tied to Location?	Easily reproducible/forwarded?
Syndromic Surveillance	Awareness of health sector	**Varies**				
HSIN	Information sharing across jurisdictions and between levels of government – initial and continuing actions as well as mapping to support a COP	**Text**	N	Y	Y	Y
GIS	Identification and analysis of assets utilizing a geographical representation	**Data**	Y	Y	Y	Y
GPS	Asset tracking as well as monitoring of various operational activities	**Data**	Y	Y	Y	Y
Plume Modeling	Situational awareness and forecasting of CBRN releases	**Data**	Y	Y	Y	Y
HAZUS	Risk assessment and damage assessment information	**Data**	Y	Y	Y	Y

SYSTEM	INFORMATION DESCRIPTION	COMMUNICATION MEDIA	Capabilities			
			Searchable?	Stored?	Tied to Location?	Easily reproducible/forwarded?
SLOSH	Storm surge assessments and forecasting along the nation's coastlines	**Data**	Y	Y	Y	Y
E-mail	Information sharing both internally and externally for EOC personnel	**Voice/Text/Video**	Y	Y	N	Y

Y – Yes
N – No
S – Sometimes

The task of expanding the capabilities for many of the above systems is not impossible. Many of the current CIMS have already incorporated the above technologies, and the integration of any system would likely require a legacy system to be supported by a digital format for any integration.

X.   CONNECTING ALL THE PIECES

A regional or national CIMS could be developed to connect information management systems being utilized within jurisdictions by connecting them through a portal. To control access to sensitive information within an EOC, each jurisdiction would create a shared space within its current IT infrastructure. Only information within the shared space would be accessible to the portal and other jurisdictions. Figure 7 illustrates how this system might be configured.
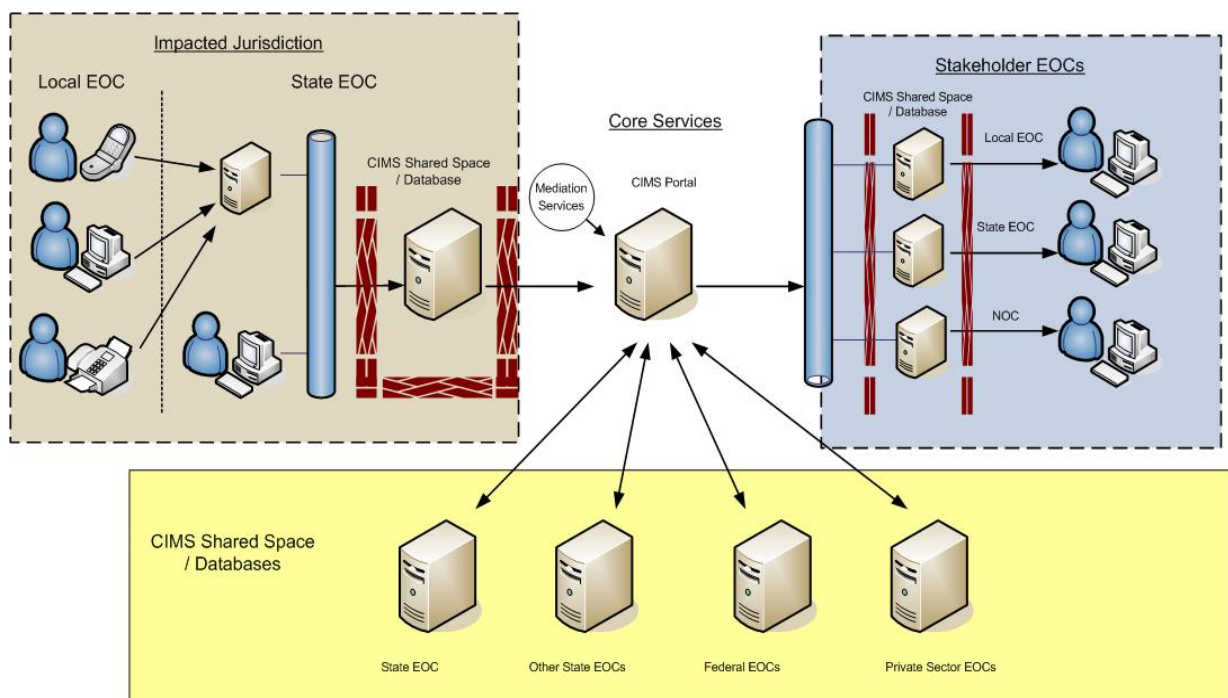

Figure 7.   A National Crisis Information Management System

The portal identified in Figure 7 shows an enhancement over the current information-sharing and interoperability systems by reducing the current labor-intensive efforts of calling and logging into multiple systems and then manually compiling the information into a single document for dissemination. By streamlining this process with a portal, emergency response equipment and activities can be identified and reported in a

timely manner. Quicker identification and movement of resources into ravaged New Orleans after Hurricane Katrina, as well as a better understanding at the federal level of the response by local officials, may have saved lives and reduced injury.

Crisis Information Management Systems (CIMS) are often defined as the software commonly found in emergency operation centers that support the management of crisis information and the corresponding response by public safety agencies.[125] When used to their full potential, CIMS can increase first responders' operational response and situational awareness, and can help central command and control facilities communicate and coordinate the activities of multiple agencies, preventing delays, confusion, and ineffective responses. These programs also have been used as platforms to integrate other systems, allowing for EOCs to manage all aspects of a disaster using a single system.

The purpose of Homeland Security Presidential Directive (HSPD) 8 is to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive National Incident Management System (NIMS).[126] Incidents typically begin and end locally, and are managed on a daily basis at the lowest possible geographical, organizational, and jurisdictional level. However, there are instances in which successful incident management operations depend on the involvement of multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines.[127] For multiple jurisdictions and agencies to work together to respond to an emergency, it is critical they have the tools to manage emergencies across jurisdictions and not just with other jurisdictions. Crisis Information Management Systems support many objectives identified in HSPD 8 for states, but adding a portal to connect state and local IT infrastructure with other states and the federal government would improve information sharing and interoperable communications.

---

[125] Department of Justice, "Crisis Information Management Software (CIMS) Feature Comparison Report."

[126] The White House, "Homeland Security Presidential Directive/HSPD-8," February 28, 2003, http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html (accessed November 2007).

[127] Federal Emergency Management Agency, "National Incident Management System."

XI. BRINGING STRUCTURE TO THE SYSTEM

One concern about HSIN is over the posting of information and whom has access to the information posted.[128] With approximately 18,000 users, many persons with the ability to post wish they had more control over who could view what was being posted.[129]

Any successful information-sharing approach utilized across the country and between levels of government should utilize a known organizational structure. The use of a known structure could allow for the identification of groups to improve information management.

The National CIMS should be consistent with the Incident Command System (ICS). ICS is the model tool for command, control, and coordination of a response, and is built around five major management activities of an incident.[130]

- Command
- Operations
- Planning
- Logistics
- Finance/administration.

The new system should also be consistent with the National Response Plan and the Emergency Support Functions (ESF). These fifteen support functions cover all activities that would support an emergency response and have clearly identified roles and responsibilities at the federal level. Most states also utilize an ESF structure, allowing for coordination between local, state and federal government when supporting a particular ESF.

Each ESF identified within local, state and federal plans is headed by a lead organization responsible for coordinating the delivery of goods and services to the

---

[128] Joshua Jack, Interview with Chris Voss, September 4, 2008.

[129] Mark Gabriel, Interview with Chris Voss, September 2, 2008.

[130] Department of Justice, "Crisis Information Management Software (CIMS) Feature Comparison Report," 6.

disaster area and is supported by numerous other organizations. The value of an ESF structure is two-fold: it provides a recognizable structure for many emergency responders working in EOCs, and it will allow for easier collection and dissemination of information than a general situational log, which compiles all information into the same place. The ESF annexes are as follows.

- ESF #1 - Transportation
- ESF #2 – Communications
- ESF #3 - Public Works and Engineering
- ESF #4 - Firefighting
- ESF #5 - Emergency Management
- ESF #6 - Mass Care, Housing, and Human Services
- ESF #7 - Resource Support
- ESF #8 - Public Health and Medical Services
- ESF #9 - Urban Search and Rescue
- ESF #10 -Oil and Hazardous Materials Response
- ESF #11 -Agriculture and Natural Resources
- ESF #12 -Energy
- ESF #13 -Public Safety and Security
- ESF #14 - Long-Term Community Recovery and Mitigation
- ESF #15 -External Affairs

Applying an organizational structure to a regional or national CIMS could allow users to improve the dissemination of information to targeted groups, improve the search for relevant information on a specific incident, and may also improve the willingness of users to share information.

The dissemination of information can be improved simply by allowing persons who are posting information to choose the groups to which they wish to disseminate information. With 18,000 users able to post information, a large number of users blanketing the system with information might quickly overwhelm the system. Organizing information based on Emergency Support Function will be one step in managing information.

58

If users posted information to support a specific Emergency Support Function, it would reduce the task of searching through entire documents to find information on a specific activity or process. As many Situation reports are developed and organized by ESF, this approach could allow law enforcement to view and monitor law enforcement activities only rather than sifting through information from fourteen other disciplines.

All levels of government have concerns over the security of information. These concerns include who has access to the information, to whom they might send the information, what decisions are made with the information, and if a national CIMS portal was developed, and whether a reduction in the access and integrity of the system cause more harm than good. There is also a cultural hesitancy among emergency managers and other disciplines when information is disseminated to large unknown audiences. Owners of information want to control who sees their data and to whom it may be sent.[131] Responders will be hesitant in sending sensitive information to someone they do not personally know, regardless of the security of the transmission medium.[132] An organizational structure could improve the level of trust between users if the portal allowed the person in control of the information to choose who was to gain access. Factors should include geographical area, level of government and ESF. Options for sharing information for a single local jurisdiction should include the following.

- One Discipline, Select Disciplines or all Disciplines within a jurisdiction
- One Discipline, Select Disciplines or all Disciplines within a regional area
- One Discipline, Select Disciplines or all Disciplines throughout the country
- One Discipline, Select Disciplines or all Disciplines supporting a specific level of government (federal, state and/or local)

---

[131] Department of Justice, "Crisis Information Management Software (CIMS) Feature Comparison Report," 2-3.

[132] Ibid., 2-3.

According to emergency managers at the local and state level, these options would increase the willingness of users to post information.[133] While these options will not eliminate concerns from jurisdictions about sharing information, they may mitigate the impact by giving the poster of information more control over what users have access.

---

[133] Josh Jack, interview with Chris Voss, September 4, 2008.

XII. CONCLUSION

The purpose of Homeland Security Presidential Directive (HSPD) 8 is to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive National Incident Management System (NIMS).[134] Incidents typically begin and end locally and are managed on a daily basis at the lowest possible geographical, organizational, and jurisdictional level. However, there are instances in which successful incident management operations depend on the involvement of multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines.[135] It is sometimes necessary for multiple jurisdictions and agencies to work together to respond to an emergency. At these times, it is critical that they have the tools to manage emergencies across jurisdictions, and not just with other jurisdictions.

One Dartmouth survey identified CIMS as both relatively interoperable and intraoperable.[136] All of the vendors in the survey said computers or servers within their CIMS program can share data with each other and the most common method of data transfer used to share data was the Internet Protocol (IP).[137] The extensible Markup Language, or XML, was the most common language for the interchange of structured data, and a majority of the systems used XML for both data import and export.[138]

A majority of CIMS use XML, but the use is not universal. One benefit of XML is that a government would not have to junk legacy systems if a national or regional CIMS were to be implemented, which is very attractive to states that have grown accustomed to their system and do not have the funding to scrap them.[139] XML makes

---

[134] The White House, "Homeland Security Presidential Directive/HSPD-8."

[135] Federal Emergency Management Agency, "National Incident Management System," 5.

[136] Dartmouth University, "Crisis Information Management Software (CIMS) Interoperability."

[137] Ibid.

[138] Ibid.

[139] Peterson, "Crime and the Tech Effect The XML Factor."

sharing that information with other entities easy and relatively cheap because it is a Web-based technology, but this would also mean jurisdictions not using an XML would need additional funding to be integrated.[140]

The United States is at a crossroads in improving information sharing between EOCs. Integrating current systems across the country's EOC may be a more difficult task than just providing EOCs a system they can use. However, the end state is not so much having a system that people *can* use as it is having a system they *do* use. Federal resources have been utilized to create HSIN, a top down solution to improving integration across EOCs, where state and local organizations are provided access to a federal system. Knowing that many issues exist with HSIN, and that the system is not user friendly, only six percent of the users log in daily. The system is considered redundant and a burden by many state and local users, DHS has announced the desire to create a next generation HSIN, and has already awarded a contract for sixty-two million dollars to build the system.[141] The new system has not been built and already there is a wave of resentment and calls for DHS to address "user's needs," which the original HSIN never did.[142]

The nation can continue to spend millions for these systems or it can make efforts to integrate the systems in use every day. This paper identifies a path for success, which includes improving the systems now in use, integrating those systems throughout EOCs in the country, and allowing users to maintain control over their information and how and to whom it is shared. If DHS acknowledges the lessons from deploying HSIN, it will take a different approach and will not create a newer version of the same system. Currently, DHS appears to have a total lack of consideration of user needs and a misunderstanding of people's disaffection for the current system. The disconnect at DHS with current state and local operations can be further viewed in the naming of the new system after the old one. Months after the Titanic sank, who would want to take a ride on

---

[140] Peterson, "Crime and the Tech Effect The XML Factor."

[141] FCW.COM, "DHS Official Defends HSIN Next Gen," http://www.fcw.com/online/news/153348-1.html (accessed September 2008).

[142] Ibid.

Titanic II? Anyone want to invest in Enron II? The use of the old name is likely to alienate many of the same users who need access and must use the system to be successful.

The choice is clear. The United States has hundreds, if not thousands, of emergency operation centers at the local, state and federal government level. Individually, many of these EOCs have implemented systems to help manage and integrate systems throughout their jurisdictions. In much the same way as the nation made it a priority for first responders to be able to communicate with each other when responding to an emergency, so must it become a priority for EOCs to be able to communicate with one another across all levels of government by connecting state and local CIMS already being used on a daily basis.

CIMS, when used to its full potential, can increase first responders' operational response and situational awareness and can help central command and control facilities communicate and coordinate the activities of multiple agencies preventing delays, confusion, and ineffective responses. These programs also have been used as platforms to integrate other systems allowing for EOCs to manage all aspects of a disaster using a single system.

A regional or national CIMS would improve interoperability between EOCs and would support development of a common operating picture for catastrophic disasters, information dissemination, resource requests and management at a national level. Connecting the nation's CIMS would also provide a platform with which to integrate future systems rather than to create stand-alone systems. In short, connecting the nation's CIMS will ensure that we are better prepared to respond to catastrophic events as a nation.

In 2002, the National Institute for Justice performed a survey of CIMS systems and concluded the following.

- There is no best product
- There is no perfect fit
- There is only a best product for each agency based on

- System environment
- Scale of operation
- Sophistication of operation
- Discipline to implement
- Political considerations[143]

The federal, state and local governments should cease trying to find the one system that will work for everyone, and instead, improve and connect the information sharing and CIMS in use every day. With this approach, jurisdictions will not just have integration, but will also be willing to use it.

---

[143] Department of Justice, "Crisis Information Management Software (CIMS) Feature Comparison Report," 18-19.

LIST OF REFERENCES

9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton & Co, 2004, http://www.9-11commission.gov/report/911Report.pdf (accessed November 2007).

Association of State and Territorial Health Officials. *A Summary of Four After-Action Reports on Hurricane Katrina*. May 9, 2006, http://www.astho.org/pubs/KatrinaReportsSummary.pdf (accessed November 2007).

Barbaro, Michael and Justin Gillis. *Walmart at Forefront of Hurricane Relief*. The Washington Post, September 6, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/09/05/AR2005090501598.html (accessed December 2007).

Dartmouth University. Institute for Security Technology Studies. *Crisis Information Management Software (CIMS) Interoperability*. October 2004, http://www.ists.dartmouth.edu/projects/archives/cims1004.pdf (accessed December 2007).

Davis, Fred D., et al. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models." *Management Science* 35, no. 8 (1989): 982.

Emergency Management Assistance Compact. "EMAC FAQ." http://www.emacweb.org/?10#Why%20should%20my%20state%20join%20EMAC? (accessed September 2007).

Emergency Management Assistance Compact. "The History of Mutual Aid and EMAC." http://www.emacweb.org/?321 (accessed September 2007).

Emergency Management Assistance Compact. "How Does EMAC Work?" http://www.emacweb.org/?142 (accessed September 2007).

Federal Emergency Management Agency. "FEMA History." Federal Emergency Management Agency. http://www.fema.gov/about/history.shtm (accessed November 2007).

Federal Emergency Management Agency. "National Incident Management System." Federal Emergency Management Agency. August 2007, http://www.fema.gov/library/viewRecord.do?id=2961 (accessed November 2007).

National Weather Service. *Policy References National Warning System.* National Weather Service. http://www.srh.noaa.gov/cwwd/faqs/nawas.htm (accessed September 2007).

Peterson, Shane. "Crime and the Tech Effect The XML Factor." *Government and Technology.* (March 7, 2003), https://www.chds.us/courses/file.php/244/Readings/Winter_07/1-XML_Factor.pdf (accessed November 2007).

U.S. Department of Homeland Security. "Homeland Security Information Network Factsheet." Department of Homeland Security. http://www.dhs.gov/xnews/releases/press_release_0418.shtm (accessed November 2007).

U.S. Department of Homeland Security. "Interim National Preparedness Goal." March 31, 2005, http://www.ojp.usdoj.gov/odp/docs/InterimNationalPreparednessGoal_03-31-05_1.pdf (accessed December 2007).

U.S. Department of Homeland Security. *National Strategy for Homeland Security.* Washington, D.C.: U.S. Government Printing Office, July 2002.

U. S. Office of Homeland Security. *The National Response Plan.* Washington, D.C.: Government Printing Office, December 2004.

United States. The White House. "Homeland Security Presidential Directive/HSPD-5." February 28, 2003, http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html (accessed November 2007).

United States. The White House. *Homeland Security Presidential Directive/ HSPD-8*: *National Preparedness*. December 17, 2003. Washington, D.C.: Government Printing Office, 2003.

United States. The White House. *The Federal Response to Hurricane Katrina: Lessons Learned*. (Foreword by Frances Townsend, Assistant to the President for Homeland Security and Counterterrorism) February 23, 2006. Washington, D.C.: Government Printing Office, 2006.

Wailgum, Thomas. "How Wal-Mart lost its Technology Edge." CIO. http://www.cio.co.uk/concern/resources/features/index.cfm?articleid=517&pagtype=allchandate (accessed December 2007).

INITIAL DISTRIBUTION LIST

1.   Defense Technical Information Center
        Ft. Belvoir, Virginia

2.   Dudley Knox Library
        Naval Postgraduate School
        Monterey, California